Rooks Heath College

Data Protection Policy

Introduction

This policy replaces any previous policy and follows the DfE regulations.

In line with the college's Equal Opportunities and Special Educational Needs policies, we aim to give all students equal opportunities to take part in all aspects of college life, as far as is appropriate, practicable and compatible with giving regard to health and safety and the efficient education of other students.

This policy takes account of the Government's aim for children to have the support they need under Every Child Matters:

- to be healthy
- to stay safe
- to enjoy and achieve
- to make a positive contribution
- to achieve economic well-being

The policy will follow the five principles of the Children's Plan:

- to support parents and families
- to allow children to reach their full potential
- to enable children to enjoy their childhood whilst preparing for adult life
- to provide services in response to children and family needs
- to use preventative measures to help students avoid the possibility of failure

This policy is based upon the College's commitment to the development and maintenance of good behaviour and a positive and inclusive ethos for all members of the College community.

Revised Edition: April 2015
Ratified by Governors: 18th June 2015
To be reviewed bi-annually by the Associate Headteacher/Network Manager

Foreword

Rooks Heath College is a mixed 11 to 18 multicultural comprehensive in the London Borough of Harrow. This policy is formulated by the Associate Headteacher and the Network Manager. It is monitored by other members of the college's Leadership and Management Group. The policy is subject to bi-annual review by the college's Leadership and Management Group and is subject to approval by the governors of the college.

Introduction

Rooks Heath collects and uses personal information about staff, students, parents and other individuals who come into contact with the college. This information is gathered in order to enable it to provide education and other associated functions. Data can be stored in many places, including the College network or the Cloud. It can be used, not only by college employees, but also relevant agencies, such as the local authority. In addition, there may be a legal requirement to collect and use information to ensure that the College complies with its statutory obligations.

All schools have a duty to be registered, as Data Controllers, with the Information Commissioner's Office (ICO) detailing the information held and its use. These details are then available on the ICO's website. Our registered no. is 00041029540. Schools also have a duty to publish Privacy Notices to all students/parents, as well as staff. These summarise the information held and why it is held and the other parties to whom it may be passed on. The 'Privacy Notice – students' is available on the College website.

Purpose

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the Data Protection Act 1998, and other related legislation. It will apply to information regardless of the way it is collected, used, recorded, stored and destroyed, and irrespective of whether it is held in paper files or electronically.

All staff involved with the collection, processing, disclosure and disposal of personal data will be aware of their duties and responsibilities by adhering to these guidelines. Please see the Data Protection Staff Handbook for further details.

Personal Information *(Appendix 1)*

Personal information or data is defined as data which relates to a living individual who can be identified from that data, or other information held.

Good practice in Information Handling

- All data will be kept safe and made available only to those who are authorised to access it.

- Where sensitive or personal data is removed from the college premises the media used will be encrypted and it will be transported securely for storage in a secure location.
- When data is required by an authorised user from outside the college premises – for example, by a teacher working from home – he/she will have secure remote access to the management information system or learning platform, where this is available.
- All desktop, portable and mobile devices (including media) used to store and transmit personal information, using approved encryption software, will be protected.
- Sensitive or personal data will be deleted when it is no longer required.
- Unless requested otherwise, passwords given to Parents/Carers will be issued either directly or by post.

The right of individuals to access personal information *(Appendix 2)*

Under data protection legislation, individuals have a right to know what information is held about them. The ICO provides a framework to ensure that personal information is handled properly.

Data Protection Principles *(Appendix 3)*

The Data Protection Act 1998 establishes eight enforceable principles that must be adhered to at all times:

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes
3. Personal data shall be adequate, relevant and not excessive
4. Personal data shall be accurate and where necessary, kept up to date
5. Personal data processed for any purpose shall not be kept for longer than is necessary for that purpose or those purposes
6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act 1998
7. Personal data shall be kept secure i.e. protected by an appropriate degree of security
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

Rooks Heath is committed to maintaining the above principles at all times. Therefore the College will:

- Inform individuals why the information is being collected when it is collected
- Inform individuals when their information is shared, and why and with whom it was shared, unless it is an exempt item under the Data Protection Act, such as issues relating to child protection
- Check the quality and the accuracy of the information it holds
- Ensure that information is not retained for longer than is necessary
- Ensure that when obsolete information is destroyed that it is done so appropriately and securely
- Ensure that clear and robust safeguards are in place to protect personal information from loss, theft and unauthorised disclosure, irrespective of the format in which it is recorded
- Share information with others only when it is legally appropriate to do so
- Set out procedures to ensure compliance with the duty to respond to requests for access to personal information, known as Subject Access Requests
- Ensure that staff are aware of and understand our policies and procedures.

Security

All personal data will be protected by passwords. Staff will be expected to keep passwords secure and follow advice given by the ICT team/Associate Headteacher. Simple passwords should never be used by staff.

All members of staff should be constantly aware of the possibility of personal data being seen by unauthorised personnel. All papers, containing student data, must be kept securely. College computers screens lock out after being left for 2 minutes.

Freedom of Information

Any member of staff receiving a freedom of information request, should pass this request to the Associate Headteacher and the Director of Business without delay. Such requests will then be processed within 15 working days.

Consent

When a student joins the College, written consent is sought for biometric scanning of the finger. This is used for purchasing of lunch and to take books out of the library. Written consent is also obtained for photographs, films and digital images of the student to be used in publications and web pages produced by the College.

Provision of Data

It is a criminal offence to knowingly or recklessly obtain or disclose information about an individual without legitimate cause. Relevant, confidential data should only be given to:

- Other members of staff on a need to know basis.
- Relevant Parents/Carers.
- Other authorities if it is necessary in the public interest, e.g. prevention of crime.
- Other authorities, such as an LA and schools to which a student may move and where there are other legitimate requirements.

The College should not disclose anything on a student's record which would be likely to cause serious harm to their physical or mental health or that of anyone else. Therefore, those who create such records should ensure that such information is separated from other records.

Where there is doubt or statutory requirements conflict advice should be obtained. When giving information to an individual, particularly by telephone, it is most important that the individual's identity is verified. If in doubt, questions should be asked of the individual, to which only he/she is likely to know the answers. Information should not be provided to other parties, even if related. For example: in the case of divorced parents it is important that information regarding one party is not given to the other party to which he/she is not entitled.

Disposal of Data

When a student or employee leaves, data will be retained only according to DfE guidance. After this time, it will be destroyed. This may mean that paper records are shredded, electronic records are securely deleted and CCTV tapes wiped clean. Photographs used for publicity will also be removed and destroyed after the appropriate time. Staff responsible for the disposal of data will have this written in their job descriptions. The Headteacher has overall responsibility for ensuring this happens.
All employees who keep their own records containing personal data about staff, parents or students, must ensure that the data is destroyed when it is no longer relevant.

Breach of this Policy

Non-compliance with the requirements of this policy by a member of staff could lead to serious action being taken by third parties against the College. Non-compliance by a member of staff is therefore considered a disciplinary matter that, depending on the circumstances, could lead to dismissal. It should be noted that an individual can commit a criminal offence under the Data Protection Act, for example, by obtaining and/or disclosing personal data for his/her own purposes without the consent of the College. Anybody who suspects there has been a breach to this policy, should report it to the Associate Headteacher and Director of Business.

Complaints

Complaints will be dealt with in accordance with the College's Complaints policy. Complaints relating to information handling may be referred to the Information Commissioner (the statutory regulator).

Contacts

Further advice and information is available from the Information Commissioner's Office, www.ico.gov.uk or telephone 01625 545745 3

Appendixes

1. What is personal data?
2. Procedures for responding to subject access requests.
3. Data Protection Principles.

Appendix 1

What is personal data?

The Information Commissioner's Office (ICO) defines personal data as:

- Information processed, or intended to be processed, wholly or partly by automatic means (information in electronic form such as on a computer)
- Information processed in a non-automated manner, which forms part of, or is intended to form part of, a 'filing system' (usually paper records)
- Information that forms part of an 'accessible record' (educational records) regardless of whether it is processed automatically or is held in a filing system
- Information held by a public authority

An ICO guidance document outlines a number of questions to enable staff to identify personal data. They include:

1. Can a living individual be identified from the data, or from the data and other information in the possession of, or likely to come into the possession of, the data controller? This can be a name, or a name combined with an address or telephone number. A name does not always have to be present; for example, a combination of gender, age and address could make someone identifiable
2. Does the data 'relate to' the identifiable living individual, whether personal, or family life, business or professional?
3. Is the data 'obviously about' a particular individual? This can be someone's medical history, a criminal record, or an individual's performance
4. Is the data 'linked to' an individual so that it provides particular information about that individual?
5. Is the data used, or is it to be used, to inform or influence actions or decisions affecting an identifiable individual?

What is sensitive personal data?

Sensitive personal data is defined as:

- The racial or ethnic origin of the data subject
- His/her political opinions
- His/her religious beliefs or other beliefs of a similar nature
- Whether he/she is a member of a trade union (within the meaning of the [1992 c. 52.] Trade Union and Labour Relations (Consolidation) Act 1992)
- His/her physical or mental health or condition
- His/her sexual life
- The commission or alleged commission by him/her of any offence

- Any proceedings for any offence committed or alleged to have been committed by him/her, the disposal of such proceedings or the sentence of any court in such proceedings

Appendix 2

Rooks Heath College

Procedures for responding to subject access requests made under the Data Protection Act 1998

Rights of access to information

There are two distinct rights of access to information held by schools about students.

1. Under the Data Protection Act 1998 any individual has the right to make a request to access the personal information held about them.

2. The right of those entitled to have access to curricular and educational records as defined within the Education Pupil Information (Wales) Regulations 2004.

Actioning a subject access request

1. Requests for information must be made in writing; which includes email, and be addressed to the Headteacher. If the initial request does not clearly identify the information required, then further enquiries will be made.

2. The identity of the requestor must be established before the disclosure of any information, and checks should also be carried out regarding proof of relationship to the child. Evidence of identity can be established by requesting production of:
    - passport
    - driving licence
    - utility bills with the current address
    - Birth / Marriage certificate
    - P45/P60
    - Credit Card or Mortgage statement

This list is not exhaustive.

3. Any individual has the right of access to information held about them. However with children, this is dependent upon their capacity to understand (normally age 12 or above) and the nature of the request. The Headteacher should discuss the request with the child and take their views into account when making a decision. A child with competency to understand can refuse to consent to the request for their records. Where the child is not deemed to be competent an individual with parental responsibility or guardian shall make the decision on behalf of the child.

4. The College may make a charge for the provision of information, dependent upon the following:
    - Should the information requested contain the educational record then the amount charged will be dependent upon the number of pages provided.

- Should the information requested be personal information that does not include any information contained within educational records schools can charge up to £10 to provide it.

- If the information requested is only the educational record viewing will be free, but a charge not exceeding the cost of copying the information can be made by the Headteacher.

5. The response time for subject access requests, once officially received, is 40 days (not working or school days but calendar days, irrespective of school holiday periods). However the 40 days will not commence until after receipt of fees or clarification of information sought

6. The Data Protection Act 1998 allows exemptions as to the provision of some information; **therefore all information will be reviewed prior to disclosure**.

7. Third party information is that which has been provided by another, such as the Police, Local Authority, Health Care professional or another school. Before disclosing third party information consent should normally be obtained. There is still a need to adhere to the 40 day statutory timescale.

8. Any information which may cause serious harm to the physical or mental health or emotional condition of the pupil or another should not be disclosed, nor should information that would reveal that the child is at risk of abuse, or information relating to court proceedings.

9. If there are concerns over the disclosure of information then additional advice should be sought.

10. Where redaction (information blacked out/removed) has taken place then a full copy of the information provided should be retained in order to establish, if a complaint is made, what was redacted and why.

11. Information disclosed should be clear, thus any codes or technical terms will need to be clarified and explained. If information contained within the disclosure is difficult to read or illegible, then it should be retyped.

12. Information can be provided at the school with a member of staff on hand to help and explain matters if requested, or provided at face to face handover. The views of the applicant should be taken into account when considering the method of delivery. If postal systems have to be used then registered/recorded mail must be used.

Further advice and information can be obtained from the Information Commissioner's Office, www.ico.gov.uk or telephone

Appendix 3
Data Protection Principles

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless:-

   (a) at least one of the conditions in Schedule 2 is met, and

   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

   In practice, it means that you must:

   - Have legitimate grounds for collecting and using the personal data.
   - Not use the data in ways that have unjustified adverse effects on the individuals concerned.
   - Be transparent about how you intend to use the data, and give individuals appropriate privacy notices when collecting their personal data.
   - Handle people's personal data only in ways they would reasonably expect; and make sure you do not do anything unlawful with the data.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.

4. Personal data shall be accurate and, where necessary, kept up to date.

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

6. Personal data shall be processed in accordance with the rights of data subjects under this Act.

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

   In practice, it means you must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, you will need to:

•design and organise your security to fit the nature of the personal data you hold and the harm that may result from a security breach;

•be clear about who in your organisation is responsible for ensuring information security;

•make sure you have the right physical and technical security, backed up by robust policies and procedures and reliable, well-trained staff; and

•be ready to respond to any breach of security swiftly and effectively.

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.